DEPARTMENT OF THE AIR FORCE
HQ AIR INTELLIGENCE AGENCY

70TH INTELLIGENCE WING INSTRUCTION 31-402

1 December 2000

Security

INFORMATION SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: 70 IW/SF (SMSgt Norman)

Certified by: 70 IW/CC (Col Beatty)
Pages: 12
Distribution: X

This operating instruction applies to all military members, reservists (including IMAs), DoD civilians, and contractors assigned to, on temporary duty to, or visiting the 70 IW and/or one of its subordinate units. This instruction identifies the procedures associated with the completion of a preliminary inquiry/investigation. Each Intelligence Group Security Forces Section will supplement this instruction, where necessary, through guidance set forth in the unit's Information Security Operating Instruction or as a stand alone Operating Instruction.

1. **GENERAL:** It is the responsibility of every assigned, attached or visiting member to properly safeguard classified information entrusted to him/her and to report, immediately, instances of suspected compromise or known risk that pose a threat to the integrity of the Information Security Program. In the event of a suspected compromise or risk to classified material, the person(s) discovering the incident must take control of the material(s) and safeguard them until the material(s) can be properly stored. Notification of the incident must be reported to the servicing Security Forces Office.

2. **SECURITY INCIDENTS AND COMPROMISES:**

2.1. **Introduction**:

2.1.1. DoD Directive 5200.1, DoD Manual 5105.21-M-1 and AFI 31-401 outline the basic requirements for handling security incidents involving security violations.

2.1.2. The compromise of classified information presents a serious threat to national security. Compromises not only affect the security of our country, they also impact our foreign policies. To prevent damage to national security and foreign policy, all security violations involving classified information are investigated.

2.1.3. Take appropriate action to educate and, where necessary, discipline personnel that violate established security policy.

2.2. **Explanation of Terms**: The following terms are commonly used in preliminary inquiries and formal investigations:

2.2.1. Access: The ability and opportunity to obtain knowledge of classified information. Individuals in fact may have access to classified information by being in a place where such information is kept and the security measures that are followed do not prevent them from gaining knowledge of such information.

2.2.2. Accused: One who has been made a subject of a formal charge.

2.2.3. Appointing Authority: The Group's Senior Intelligence Officer, who appoints, in writing, an official to conduct an inquiry or investigation.

2.2.4. Administrative Sanctions: Nonjudical action, which may be taken against any military or civilian employee who violates the provisions of applicable DoD and Air Force guidance.

2.2.5. Classified Information: Information or material that is owned by, produced for or by, or is under the control of the US Government and determined under Executive Order 12958 (or prior executive order) and DoD Directive 5200.1/AFI 31-401 to require protection against unauthorized disclosure.

2.2.6. Compromise: The disclosure of classified information to persons not authorized access.

2.2.7. Complainant: One who makes a formal allegation against another person or activity.

2.2.8. Formal Investigation: A determination of the facts surrounding a particular event, occurrence, circumstance, or action. For the purpose described in this instruction, a formal investigation requires a written report and record of action taken by proper authority as a result of the investigation. Investigations are supported by exhibits and sworn testimony of witnesses.

2.2.9. Inquiry: A determination of the facts of a matter by checking records, reviewing applicable directives, examining material evidence, and interviewing persons with a direct knowledge of a particular matter. Such processes are generally adequate if the inquiry is not complex or of serious consequence and the matter can be resolved through normal staff functions and procedures. For the purpose described in this instruction, a preliminary inquiry requires a written report and action taken by proper authority as a result of the inquiry.

2.2.10. Investigator: Any commissioned officer, senior noncommissioned officer (Master Sergeant through Chief Master Sergeant), or civil service employee holding an equivalent grade (GS-9 or above) that is detailed by an appointing authority to conduct an inquiry or investigation.

2.2.11. Information Security Program Manager (ISPM): The senior security police official at each command or installation.

2.2.12. National Security Information: Information associated with the national defense and foreign relations of the United States.

2.2.13. Practice Dangerous to Security: A failure to comply with the provisions of security regulations or this manual, which causes a potential compromise of classified information.

2.2.14. Probable Compromise: An incident in which a reasonable presumption exists that an unauthorized person had or has access to classified information.

2.2.15. Responsible Custodian: Person charged with the protection and maintenance of a classified document.

2.2.16. Suspect: An individual who, considering all the facts and circumstances at the time of the interview, is believed to have committed an offense. The offense may be a violation of the Uniform Code of Military Justice, for example, Article 92, Dereliction of Duty, or other federal statutes.

2.2.17. Witness: Anyone called to appear during an inquiry or investigation.

2.2.18. Security Incident: A violation of the information security program standards or procedures that requires an investigation and that a compromise determination be made.

2.3. **Responsibility of the Discoverer**: The discoverer of a security incident takes measures to protect the classified material and report the situation to a security authority. This authority may be his/her security manager, immediate supervisor, or commander in the discoverer's chain of command. The classified material is protected until it can be released to the responsible custodian or other proper authority. Once accomplished, the discover's responsibility for the classified material is relinquished. The unit commander responsible for the classified material ensures that the incident is reported to the servicing Security Forces office NLT the next duty day.

2.4. **Special Security Officer (SSO)**:

2.4.1. Ensures that the Appointing Authority is made aware of the security incident so that an inquiry official can be appointed and a quick, but thorough inquiry may be conducted.

2.4.2. Notifies 70 IW/SF no later than (NLT) the next duty day.

2.4.3. Assigns a local case number (in those instances where the incident involves collateral classified information) to the incident. Refer to the assigned case number in all subsequent correspondence, reports of inquiry, and formal investigation reports. If the security incident involves Sensitive Compartmented Information (SCI), HQ AIA/SO will be contacted and a case number requested.

2.4.4. Monitors the progress of the inquiry or investigation and provides technical guidance as needed to the inquiry official. Reviews all inquiry or investigation reports for adequacy under the provisions of DoD Directive 5200.1/AFI 31-401 and DoD Manual 5105.21-M-1. Inquiries or investigations not considered adequate are returned to the inquiry or investigation official with instructions for corrective action.

2.4.5. Ensures that the appointing authority closes the investigation (involving collateral classified information) and that corrective actions are put into place to preclude the reoccurrence of the events leading up to the security incident. In those instances when SCI is involved, the appointing authority only recommends closure. Final closure authority rest with HQ AIA/SO.

2.4.6. Ensures that 70 IW/SF is an addressee on all correspondence with HQ AIA/SO pertaining to the security incident.

2.5. **Appointing Authority Responsibilities**:

2.5.1. Appoints, in writing, a disinterested official (within the grade requirements) to conduct an expeditious and thorough inquiry or investigation whenever a security incident occurs. The inquiry or investigation becomes the primary duty of the appointed individual until the appointing authority closes the inquiry or investigation. In those instances involving SCI, the appointed official is relieved of his/her responsibility when the appointing authority recommends closure. Commanders must consider the following guidelines when selecting an inquiry or investigating official.

2.5.1.1. Unit security mangers and security office personnel must not be appointed as inquiry or investigation officials because they have defined security responsibilities which may come under scrutiny during the inquiry or investigation.

2.5.1.2. To prevent possible allegation of biased reporting, do not appoint an inquiry official or investigator from the same office where the security incident occurred.

2.5.1.3. Appoints an inquiry or investigation official with a security clearance equal to or greater than the level of the information involved in the security incident.

2.5.2. Ensures that the final inquiry or investigation report has been reviewed by the Security Forces office prior to closure.

2.5.3. Closes preliminary inquiries by completing all or a combination of the following actions: (Note: Inquiries/Investigations involving SCI must be closed by HQ/AIA/SO)

2.5.3.1. Directs remedial training to correct noted problems.

2.5.3.2. Accepts the conclusion and recommendations of the inquiry official either in whole or in part. Takes administrative or disciplinary action against those who were responsible for the security incident when warranted.

2.5.3.3. Debriefs the individuals in cases of inadvertent access and/or disclosure.

2.5.3.4. Relieves the activity of accountability for the information involved and transferring that material to another activity when the security deviation was caused by failure to properly document disposition of material.

2.5.3.5. Revises any deficient procedures or issue new procedures (if required). Take any other action necessary to prevent recurrence of the security incident.

2.5.4. Initiates an investigation to determine the circumstances surrounding the incident under DoD Directive 5200.1/AFI 31-401 and DoD Manual 5105.21-M-1, if as a result of an inquiry, a determination is made that a known compromise has occurred.

2.5.5. Ensures that a post-investigation report (summary of findings and actions taken) is forwarded to both HQ AIA/SO and 70 IW/SF.

2.6. **Special Investigative Requirements**:

2.6.1. When one or more of the following conditions exist, the appointing authority refers the security incident to the servicing Air Force Office of Special Investigation (AFOSI).

2.6.1.1. Cases which involve espionage, foreign intelligence agencies or criminal activity.

2.6.1.2. Incidents that suggest willful intent or those which indicate a person has intentionally and/or illicit purposes gained or attempted to gain access to classified information, can be interpreted as criminal activity, and may warrant AFOSI attention.

2.6.1.3. An AFOSI investigation does not substitute for the commander's investigation required by DoD Directive 5200.1/AFI 31-401 or DoD 5105.21-M-1. If AFOSI conducts an investigation as a result of a security violation, reference to the AFOSI investigation will be made part of the inquiry/investigation officials report.

2.7. **Purpose of an Inquiry**:

2.7.1. An inquiry is conducted to determine if classified information or material was subjected to actual or probable compromise. An inquiry establishes if classified information was lost or unauthorized personnel had access.

2.7.2. The inquiry suffices in lieu of a formal investigation if the appointing authority determines no additional "substantive" information will be obtained by conducting a formal investigation. Use of an inquiry report in lieu of an investigation report applies only when the incident does not involve North Atlantic Treat Organization (NATO) Restricted Data (RD) or foreign government information.

2.8. **Scope and Duration of an Inquiry**:

2.8.1. An inquiry is not extensive in scope; the inquiry official gathers available facts to support conclusions and recommendations:

2.8.1.2. Exhibits or other documentary evidence are not normally used in an inquiry unless considered essential to support the inquiry report.

2.8.1.3. The inquiry official must complete the inquiry within 30 duty days from receipt of the appointment letter. This period, however, may be extended for valid reasons only by the appointing authority.

2.9. **Inquiry Official Responsibilities**:

2.9.1. Obtains a briefing from the appointing authority or designated official (the SSO) to receive initial facts surrounding the incident.

2.9.2. Consults with the servicing SSO for technical guidance in conducting the inquiry. If necessary, obtains a briefing from the legal office pertaining to administering oaths, taking verbal testimony and sworn statements.

2.9.3. Determines the circumstances surrounding the possible loss, unauthorized or inadvertent disclosure of classified information, or security deviation involving the misuse or improper handling or safeguarding of classified information.

2.9.4. Questions personnel involved in the incident. If an individual becomes a suspect in the security incident, the inquiry official ensures advisement of individual rights under the Uniform Code of Military Justice (UCMJ), Article 31, for military and the US Constitution, Fifth Amendment, for civilians.

2.9.5. Keeps in mind the following guidelines during the course of the inquiry:

2.9.5.1. No incident is officially termed a compromise or otherwise until completion of the inquiry and acceptance of the report findings by the appointing authority.

2.9.5.2. The main purpose of the inquiry is to determine the category of the security incident so that measures can be put in to place that will either address damage assessment or preclude future similar violations.

2.9.5.3. Identify individuals responsible for the security incident and acts, omissions, or conditions that caused the incident.

2.9.5.4. The time limit for completing the inquiry is normally 10 duty days. Before sending the completed inquiry report to the appointing authority, coordinate the report, for technical review, with the servicing SSO.

2.10. **Conducting an Inquiry**:

2.10.1. The letter of appointment is the primary mechanism for initiating the preliminary inquiry process. The appointing authority or designated official (determined by the appointing authority, normally the SSO) presents the inquiry official with a briefing identifying the problems and all known facts surrounding the incident. Once this step has been taken, the inquiry official starts the preliminary inquiry.

2.10.2. Interview witnesses as quickly as possible while details are still fresh in everyone’s mind. The longer you wait to conduct the interview, the less exact witness testimony will be.

2.10.3. The logical starting point is to interview the person who discovered or reported the security incident.

2.10.4. Each individual questioned should be able to provide name of other individuals that may also be able to provide further information or verify information already provided.

2.10.5. There is no need to chase down witnesses. Your appointing authority, or designated representative will help you summon witnesses and provide space to conduct interviews privately.

2.10.6. It is not always necessary to swear witnesses during preliminary inquiries; however, you may have to take a written statement, using the AF Form 1168, Statement of Witness/Suspect, to support your findings.

2.10.7. Before each interview, identify yourself and explain the reason for the inquiry.

2.10.8. Caution witnesses about the official character of the inquiry and the need to refrain from discussing their testimony with other persons.

2.10.9. Distinguish between witnesses that do not appear to be other than providers of relevant information and witnesses that are suspects. Suspects must be advised of their rights against self-incrimination before questioning begins (UCMJ, Article 31, for military; the US Constitution, Fifth Amendment, for civilians).

2.10.10. Compile the facts that you have developed and prepare a written report of your findings. The inquiry report is sent to the appointing authority (after coordination with the servicing SSO). Unclassified reports are marked "FOR OFFICIAL USE ONLY" according to DoD 5400.7-R, Freedom of Information Act Program. Classified reports are marked accordingly. (Note: Every effort should be made to make the report unclassified.

3. **Preliminary Inquiry Report**

3.1. Preliminary Inquiry Report Explained. Inquiry reports are not extensive in nature. They merely recite facts in narrative form and provide commanders with conclusions and recommendations concerning a security incident.

3.2. **Report Format**: (See Attachment 1)

3.3. **Report Content**

3.3.1. **Section I-Appointing authority and SSO**

3.3.2. **Section II-Self explanatory** (Preliminary Inquiry Official)

3.3.3. **Section III-Self explanatory** (Ensure case number is identified)

3.3.4. **Section IV-Authority**. The initial paragraph of the report cites the authority for conducting the inquiry and states when, where and by whom the inquiry was conducted.

3.3.5. **Section V-Matter Investigated**. Contains a brief statement of the matter inquired into, the location of the security incident, and how the security incident was initially discovered or reported. When names of personnel are included, furnish their full name, rank and duty title.

3.3.6. **Section VI-Personnel Interviewed**. List all personnel that were interviewed by showing their rank, full name, duty title or functional address.

3.3.7. **Section VII-Facts**. This section is the heart of the entire inquiry report. It presents, in an orderly fashion, all established facts that have a bearing on the security incident. Facts are presented in chronological order with opinions and evaluation being omitted.

3.3.8. **Section VIII-Conclusion**. This section is the inquiry official's evaluation of how and why the security incident occurred, what or who caused the security incident, whether insufficient training was a factor, and whether or not a compromise occurred (this is the section where the compromise determination is stated).

3.3.8.1. **For Collateral Information (Top Secret, Secret, Confidential)**. (1) Compromise; (2) Probable Compromise; (3) No Compromise; (4) Security Deviation (there can be no question of compromise when this determination is made).

3.3.8.2. **For Sensitive Compartmented Information (SCI)**. (1) Compromise Certain; (2) Compromise Probable; (3) Compromise Possible; (4) Compromise Improbable; (5) Compromise None; (6) Practice Dangerous to Security. (Refer to DoD Manual 5105.21-M-1 for examples of each category)

3.3.9. **Section IX-Recommendations**. This section contains the inquiry official's recommendation for further action. Based upon the conclusion, the recommendations should suggest closing the incident or initiating a formal investigation. Recommendations to prevent the reoccurrence of a similar incident must also be made.

3.3.10. **Section X-Signature Block**. Self-Explanatory

3.3.11. **Section XI-Appointing Authority Endorsement**. Self-Explanatory.
(Note: Preliminary inquiries involving collateral information may be closed by the appointing authority. Only HQ AIA/SO can close preliminary inquiries involving SCI)

3.3.12. **Section XII-Report Marking**. Self-Explanatory.

3.4. **Acting on Inquiry Report**:

3.4.1. The appointing authority accepts or rejects in whole or in part the conclusions and recommendations of the inquiry official, closes the inquiry (except when it involves SCI), and takes appropriate action.

3.4.2. When there is no compromise that is expected to cause damage to national security, and there is no indication of significant security weaknesses, the appointing authority:

3.4.2.1. Takes administrative or disciplinary action (if warranted) against those responsible for the violation and conducts remedial training.

3.4.2.2. Ensures a debrief is conducted in those instances of an inadvertent access.

3.4.2.3. Ensures deficient unit or staff agency procedures or policies are corrected.

3.4.3. If classified material was compromised and there is a probability that national security has been damaged, the appointing authority:

3.4.3.1. Notifies 70 IW/SF and servicing SSO. The SSO ensures notification of agencies identified in AFI 31-401 is completed and coordinated with 70 IW/SF.

3.4.3.2. Appoints a disinterested official (SNCO or above or civilian GS-9 or above) to conduct a formal investigation.

NOTE: If the incident does not involve NATO, foreign government information or Restricted Data, and the appointing authority determines no additional "substantive" information will be obtained through a formal investigation, a preliminary inquiry may suffice in lieu of the formal investigation. The appointing authority takes local action based on finds of the preliminary inquiry and advises the OPR (of the material) that the material requires reevaluation of its classification according to DoD Directive 5200.1/AFI 31-401. Should the appointing authority decide that the preliminary inquiry report will not suffice in lieu of the investigation, a formal investigation into the security incident is initiated.

HAROLD J. BEATTY, Col, USAF
Commander

Attachment:
Preliminary Inquiry/Formal Investigation Sample Report

ATTACHMENT 1

DEPARTMENT OF THE AIR FORCE
70th INTELLIGENCE WING (AIA)
FORT GEORGE G. MEADE, MARYLAND

FOR OFFICIAL USE ONLY (**12**)

23 Oct 00

MEMORANDUM FOR 70 IW/CC (**1**)

FROM: MSgt Super Snooper (**2**)

SUBJECT: Preliminary Inquiry of Security Incident (Your Ltr, 13 Oct 00) (**3**)
Case # HQ AIA 00-10

1. Authority. A preliminary inquiry was conducted from 13 Oct 00 through 23 Oct 00 under the authority of your letter and DoD Directive 5200.1/AFI 31-401. (**4**)

2. Matter Investigated. On 12 Oct 00, a Confidential document was found unsecured and unattended in the senior staff coffee room, building 931, at approximately 0600hrs. (**5**)

3. Personnel Interviewed: (**6**)

a. Captain Walter C. Crunch, Any IG/XPI
b. SMSgt Righton T. Money, Any IG/DOO
c. TSgt Knownto Handle-Biz, Any Sq/CSS
d. AlC Wanttobe Snuffy, Any Sq/LGT
e. Mrs. Nifty Savings-Plan, Any Unit/CCE

4. Testimony provided to and observation of the inquiring official revealed: (**7**)

a. A classified document was transmitted from Any IG/XPI to Any IG/DOO on 11 Oct 00. The message is identified as 111300Oct 00, classified Confidential, with the unclassified subject: Unit Deactivation (U). According to Capt Crunch, the message was transmitted as priority precedence in support of the MAJCOM reorganization.

b. At approximately 0500hrs, 12 Oct 00, SMSgt Money received a telephone call from TSgt Handle-Biz about the subject message. Notification of classified message pick-up is routine action between Any IG and the CSS. SMSgt Money proceeded to the CSS and took possession of the message.

ATTACHMENT 1
FOR OFFICIAL USE ONLY (**12**)

c. Upon SMSgt Money's return to his duty section at approximately 0515hrs, 12 Oct 00, SMSgt Money processed the message and noted message warranted immediate action by Any Sq/LGT. SMSgt Money hand-carried the message to the senior staff coffee room, at 0530hrs, where he and AlC Snuffy normally met for coffee and daily mentoring. SMSgt Money placed the message on top of the water cooler and left the coffee room, before AlC Snuffy arrived, to get his favorite coffee cup.

d. The message was found unsecured and unprotected at approximately 0559hrs, 12 Oct 00, by TSgt Handle-Biz upon her entry in to the senior staff coffee room. The message was found on the floor next to the water cooler.

e. The senior staff coffee room is not a secure area. Everyone that normally uses the senior staff coffee room, has a Top Secret security clearance. Very few others enter the room. Although the coffee room receives contract cleaning services, the cleaning team normally arrives at 1600hrs each duty day. Mrs. Savings-Plan, who has a desk across from the coffee room entrance, did not recall seeing anyone, other than TSgt Handle-Biz, enter or leave the coffee room after SMSgt Money left it.

5. Conclusion. As a result of the testimony and of personal observation, it is concluded that: (**8**)

a. The incident occurred by unit personnel failing to follow established safeguarding procedures. Operating Instructions prohibit the introduction of classified to the senior staff coffee room.

b. SMSgt Money's haste to mentor AlC Snuffy and subsequent retrieval of his favorite coffee cup, caused the security violation.

c. The message was left unsecured and unattended for approximately 20 minutes. There is no evidence or indication that anyone, authorized or unauthorized, had access to the message.

d. The possibility of a compromise is very minimal

6. Recommendations. Recommend: (**9**)

a. Additional emphasis be placed on unit procedures, and personnel be reminded on a recurring basis of their responsibilities as it relates to safeguarding classified information.

ATTACHMENT 1
FOR OFFICIAL USE ONLY (**12**)

b. This incident be closed and categorized as a compromise improbable.

SUPER SNOOPER, MSgt, USAF (**10**)
Preliminary Inquiry Official

2 Attachments
1. Appointment Letter
2. AF Forms 1168

1ST Ind

Any IG/CC (**11**)

TO: Any Unit/SSO

1. I agree/disagree with the conclusion and recommendation(s) of the inquiry report.

PLACED N. CHARGE, Col, USAF
Commander